5. REFERENCES/BIBLIOGRAPHY

[1] Alexander Sirotkin, Metalink Broadband (2007) **Hacking Embedded Linux Based Home Appliances** linuxconf.eu

[2] Amir Moradi, Horst Görtz , Alessandro Barenghi, Christof Paar(2011) **On the Vulnerability of FPGA Bitstream Encryption against Power Analysis Attacks** Proceedings of the 18th ACM conference on Computer and communications security Pages 111-124

[3] Duc Kieu , Zhi-Hui Wang , Chin-Chen Chang , and Ming-Chu Li **A Sudoku Based Wet Paper Hiding Scheme,** International Journal of Smart Home, Vol. 3, No. 2, pp. 1-12

[4] Francois-Xavier Standaert , Gilles Piret, Neil Gershenfeld, Jean-Jacques Quisquater(2006) **SEA a Scalable Encryption Algorithm for Small Embedded Applications**, CARDIS' Proceedings of the 7th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications, Pages 222-236

[5] HoWon Kim1 , YongJe Choi1 and MooSeop Kim1(2005), **Design and Implementation of a Crypto Processor and Its Application to Security System Department of Information Security**, CIS' Proceedings of the 2005 international conference on Computational Intelligence and Security - Volume Part II Pages 1104-1109

[6] I. Branovic, R. Giorgi, E. Martinelli, **A Workload Characterization of Elliptic Curve Cryptography Methods in Embedded Environments** Publisher: Association for Computing Machinery, Pages: 27-34

[7] Josh Jaffe(2007), **A First-Order DPA Attack Against AES in Counter Mode with Unknown Initial Counter**, Published in: Proceeding CHES ' Proceedings of the 9th international workshop on Cryptographic Hardware and Embedded Systems Pages 1 - 13

[8] Junfeng Fan, Kazuo Sakiyama and Ingrid Verbauwhede, **Elliptic Curve Cryptography on Embedded Multicore Systems** Journal Design Automation for Embedded Systems Volume 12, Issue 3, pp 231-242

[9] Lejla Batina, Alireza Hodjat, David Hwang, Kazuo Sakiyama and Ingrid Verbauwhed(2006) **Reconfigurable Architectures For Curve-Based Cryptography On Embedded Micro-Controllers, Field Programmable Logic and Applications**, 2006. FPL. Page1-4

[10] Marc Joye, Pascal Paillier, and Berry Schoenmakers(2005), **On Second-Order Differential Power Analysis**, CHES' Proceedings of the 7th international conference on Cryptographic hardware and embedded systems, Pages 293-308

[11] Mike Burmester and Breno de Medeiros(2007), **RFID Security: Attacks, Countermeasures and Challenges** Proceeding ICOSSSE' Proceedings of the 6th WSEAS international conference on System science and simulation in engineering Pages 325-329

[12] Mike Hamburg, **Accelerating AES with Vector Permute** Instructions, Proceeding CHES '09 Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems Pages 18 – 32

[13] M.Sreerama Murty ; D.Veeraiah ; A.Srinivas Rao(2011)**Digital Signature and Watermark Methods For Image Authentication using Cryptography Analysis Journal:**

Signal & Image Processing **Issn:** 22293922 **EIssn:**0976710X **Volume:**2 **Issue:**2 **pages/rec.No:**170-179

[14] Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan and Srivaths Ravi(2004), **Security as a New Dimension in Embedded System Design** Proceedings of the 41st annual conference on Design automation DAC 4 Volume: 48, Issue: 1, Publisher: ACM Press, Pages: 753-760

[15] Peter Gutmann(2000)**, An Open-source Cryptographic Coprocessor** Published in: Proceeding SSYM'00 Proceedings of the 9th conference on USENIX Security Symposium - Volume 9 , Pages 8 – 8

[16] Prasanth Ganesan, Ramnath Venugopalan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu(2003), **Analyzing and Modeling Encryption Overhead for Sensor Network Nodes,** Proceeding WSNA ' Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications Pages 151 – 159

[17] Rahat Afreen1 and S.C. Mehrotra(June 2011) , **a review on elliptic curve cryptography for embedded systems**, International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, , Pp 84-103

[18] Sandeep Kumar(2007), **A Survey of Lightweight- Cryptography Implementations** IEEE Design & Test of Computers dtco-24-06-pos.3d

[19] Song Sun Zijun Yan Joseph Zambreno, Experiments in Attacking FPGA-Based Embedded Systems using Differential Power Analysis, EIT 2008. IEEE, pages 7-12.

[20] S. Murphy and M.J.B. Robshaw(2002), **Essential Algebraic Structure Within the AES** Published in: · Proceeding CRYPTO ' Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology, Pages 1-16

[21] Thomas DETTBARN(2006) **Protecting the copyright of an embedded device with cryptography**-- Electronica pp 14-17,

[22] Tim Good and Mohammed Benaissa, **AES on FPGA from the Fastest to the Smallest** Published in: · Proceeding CHES'05 Pages 427-440

[23] Vassilis Prevelakis and Angelos Keromytis(2002)**Designing an Embedded Firewall/VPN Gateway** Proceedings of the International Network Conference, Plymouth, UK

[24] Vinodh Gopal, Kirk Yap, Martin Dixon(January 2011**) Cryptographic Performance on the 2nd Generation Intel core processor family**, released at Intel Corporation,

[25] Wang Qingxian(Dec 2005), **The Application of Elliptic Curves Cryptography in Embedded Systems** . Proceedings of Second International Conference on Embedded Software and Systems